



## King's Research Portal

DOI:

[10.1080/14751798.2019.1565362](https://doi.org/10.1080/14751798.2019.1565362)

*Document Version*

Peer reviewed version

[Link to publication record in King's Research Portal](#)

*Citation for published version (APA):*

Salisbury, D. (2019). An evolving state of play? Exploring competitive advantages of state assets in proliferation networks. *Defense and Security Analysis*, 35(1), 2-22. <https://doi.org/10.1080/14751798.2019.1565362>

### **Citing this paper**

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

### **General rights**

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

### **Take down policy**

If you believe that this document breaches copyright please contact [librarypure@kcl.ac.uk](mailto:librarypure@kcl.ac.uk) providing details, and we will remove access to the work immediately and investigate your claim.

# **An Evolving State of Play? Exploring Competitive Advantages of State Assets in Proliferation Networks**

*Dr. Daniel Salisbury, Centre for Science and Security Studies, King's College London*

Abstract: Illicit procurement networks often target industry in developed economies to acquire materials and components of use in WMD and military programs. These procurement networks are ultimately directed by elements of the proliferating state and utilize state resources to undertake their activities: diplomats and missions, state intelligence networks, and state-connected logistical assets. These state assets have also been utilized to facilitate the export of WMD and military technologies in breach of sanctions. While used in most historic proliferation cases, their role has seen limited consideration in the scholarly literature. This article seeks systematically to contextualize state resources in proliferation networks, arguing that their use lies between state criminality and routine activity in support of national security. Considering the competitive advantages of these assets compared to similar resources available in the private sector, the article argues that nonproliferation efforts have caused states to change how they use these resources through an ongoing process of competitive adaptation.

Keywords: illicit trade; proliferation networks; arms trade; Iran; North Korea

## **Introduction**

As the number of countries willing to openly supply WMD-related technologies in state-to-state transfers has declined, state WMD programs have sought to acquire WMD technology using illicit procurement networks.<sup>1</sup> These are networks that target witting or unwitting industry in developed economies to acquire materials, components and know-how of use in these programs, often in breach of national regulation. While involving private sector actors—witting and unwitting suppliers, middlemen, financiers and shippers—these procurement

networks are ultimately directed by elements of the proliferating state, and therefore often utilize state resources to undertake their activities. These state-resources include diplomatic assets such as embassies, state intelligence networks, and logistical assets such as air force cargo planes. Beyond WMD procurement, these state assets have also been utilized to facilitate the import and export of WMD and military technologies in breach of sanctions, mostly to states, but also to non-state actors.

The use of these assets is a key feature of many illicit proliferation networks. In recent years, some attention has been given to the use of these assets, especially embassies, by North Korea in their WMD procurement efforts. However, these assets have been used extensively in most historic cases. Furthermore, the role of these elements has not been considered in any conceptual way in the existing academic literature. This article seeks systematically to contextualize state resources in proliferation networks. After framing the issue, it proceeds by considering several factors which must be taken into account in considering a definition of state-resources, and argues that use of state resources in these networks lies between state criminality and their routine use by states in support of national security. The competitive advantages of utilizing state diplomatic, intelligence and logistical assets are considered, relative to similar services offered by the private sector. The changing value of these assets as a result of counterproliferation efforts is also considered. The paper concludes by considering tools and opportunities to disrupt state-connected aspects of these networks.

### **Proliferation Networks and State Resources: Existing Scholarly Work**

Proliferation networks conducting illicit procurement and sales are ultimately state-directed, and therefore frequently have access to state resources. Recent North Korean activities illustrate the role state assets can, and frequently do, play. Most recently, in 2018 a German intelligence official noted that the North Korean embassy in Berlin had been used to acquire missile and nuclear related dual use goods over the previous two years.<sup>2</sup> In 2016 an advertisement to sell Lithium-6, a substance used in thermonuclear weapons, was linked to an individual formerly listed as “third secretary” at the North Korean embassy in

Beijing.<sup>3</sup> North Korean efforts to sell arms in breach of the UN embargo have also been traced back to North Korean intelligence agencies.<sup>4</sup> State-owned and operated shipping companies and airlines in North Korea have also been designated or scrutinized for their role in WMD-related and arms transfers. However, the use of state assets and resources extends far beyond these recent North Korean examples. Despite their prominence in these networks, little work has considered this phenomenon in a conceptual or systematic manner.

The existing academic literature on proliferation networks has only scraped the surface when it comes to conceptual discussion of network operations at the sub-state level. This literature has largely focused on the state-level, with states –suppliers and recipients– forming the “nodes”.<sup>5</sup> More recently, scholarship has started to address the “transactional level”, focusing on the role of, and interactions between, organizations, companies, and individuals. However, this has largely focused on the drivers of behavior of private sector actors, or has considered private sector actors alongside those knowingly working for proliferating states.<sup>6</sup>

At the transactional level, illicit trade is driven by demand. While it is the private sector which largely provides the technology to proliferation networks, the work of the middlemen who knowingly broker these illicit transactions, and the procurement requirements, are ultimately driven by the state programs they supply. Those elements of proliferation networks aware of the actual end user and uses of the technology being transferred are often state-connected, and frequently draw on state resources in their illicit transfers. Little attention has been given to these aspects of proliferation networks beyond cursory references in accounts of procurement for specific programs, and illicit trade more generally.<sup>7</sup>

In broad terms, Bunn has considered the role that corruption and corrupt state and government officials can play in protecting proliferation networks from enforcement.<sup>8</sup>

Anderson has briefly discussed the opportunities and challenges regarding the use of embassies, diplomatic immunity and diplomatic conventions –specifically the use of diplomatic pouches– in the procurement of proliferation sensitive goods, although he does not contrast those with other state resources.<sup>9</sup> Hastings’s valuable work provides the most extensive discussion, and makes the most significant conceptual contribution, discussing the role of “coordinators” in proliferation networks that have access to “state prerogatives and resources”.<sup>10</sup> He argues that coordinators that have access to these resources:

...can avoid setting up logistical support structures that are embedded in potentially hostile countries, while their control of their own means of transportation allows them to bypass legitimate commercial transportation infrastructure when they move goods.<sup>11</sup>

Through providing contrasting, historic and inter-related case studies of Pakistan’s procurement network, which benefitted from use of state resources such as embassies, diplomatic personnel and military transport planes, and Khan’s Libya and Iran networks, which had to rely on some commercial infrastructure, he argues that access to resources is the “most important factor” in determining the geography of proliferation networks.<sup>12</sup> In doing so, he portrays state resources as superior, increasing the certainty of successful transfers.<sup>13</sup> He implies that actors with access to these state resources would inevitably decide to make use of them. This is likely true, given the widespread use by proliferating states. However, both state and commercial resources and their relative advantages merit systematic consideration to further our understanding of proliferation network behavior.

The literature on the use of state resources in proliferation networks is also surpassed by a body of literature which discusses the role of states in illicit activities – from narcotics trafficking to wildlife crime. Much of this focuses on the illicit activities of specific states or elements of states, with much focusing on the illicit activities of North Korea.<sup>14</sup> Some scholarship also considers how specific state resources have been mobilized towards these

ends.<sup>15</sup> Despite great secrecy surrounding the activities of these networks, there is great scope to build upon this varied discussion to further understanding of the role and relative advantages of state resources in proliferation networks.

### **Between the Criminal State and Routine Activity**

To frame better the role of state resources in proliferation networks, this section sets out to provide a conceptual background and definitions. The section first considers in-depth the definition of state resources, second it argues that the use of state resources in proliferation networks falls between state criminality and their routine use in legitimate national security activities, and third it introduces the concepts of “competitive advantage” and “competitive adaptation”. These lenses will be used in the following section to consider the merits of different state assets relative to elements of the private sector that can fulfil similar functions, and the overall changing utility of these resources to proliferators.

### ***Defining State Resources***

The “state resources” considered in this paper are loosely defined as those resources under the direct control of the state, as well as those under varying levels of state influence, mostly operating outside of the borders of the proliferating state itself. It should also be noted that this article focuses on those resources involved in the transfer of the goods themselves, rather than providing enabling services.<sup>16</sup> Providing a definition of state resources is not simple given the multitude of differing national contexts. States that have utilized illicit trade to benefit their WMD programs have included dictatorships where many, if not close-to-all, activities within the country are overseen by the state (for example North Korea), those which have seen the development of an extensive private sector over recent decades (such as China), and democracies with market economies (for example India or Israel).

A loose typology of state and quasi-state resources is proposed.<sup>17</sup> Those listed in the left-hand column of figure 1 are clearly state-controlled – and are largely drawn from three

areas: the state’s diplomatic, intelligence and military assets. Quasi-state resources listed in the right-hand column are not under such direct control of the government, but potentially still fall under state or government influence.

**Figure 1: State and Quasi-State Resources**

State Resources	Quasi-State Resources
<u>Diplomatic</u> : Embassies, diplomats and diplomatic networks.	<u>Industrial</u> : state-owned or state-controlled procurement companies, manufacturers, their subsidiaries, and loyal middlemen.
<u>Intelligence</u> : operatives, networks and related assets.	<u>Financial</u> : state-owned or state-connected financial institutions
<u>Logistical</u> : transportation infrastructure, military and other state-controlled transportation assets.	<u>Logistical</u> : state-owned or state-connected shipping companies and airlines.

Quasi-state resources fall in a grey area that merits discussion in this section. The first two categories –“industry and “financial”– are not the focus of this article, mostly operating inside of the state procuring or exporting in the face of sanctions. “Industry” includes the state-connected industry actors involved in the procurement or sales of WMD-related and military goods. Procurement companies and their front companies based in the proliferating state are often directly linked to the WMD program and therefore arguably subject to a degree of government control. In some countries, the manufacturing base for strategic and military technologies is also closely linked to the state. These entities can also be involved in illicit procurement activities which benefits WMD programs. However, while technically “state-owned”, the day-to-day activities of these –often large and complex– organizations are not directly overseen by the state.<sup>18</sup>

The middlemen or procurement agents operating overseas often form part of the private sector, although they can also have connections to the state – the degree to which this is the case varies. At the very least, procurement agents are privy to the state WMD program’s procurement requirements, either directly, or through proxy, viewing tenders and sending out “requests for quotes” to suppliers, although they may also be unaware of the end use. Many of these individuals also have other connections to the state –either being an agent of the proliferating state, having an ideological affiliation, or simply sharing nationality. Those involved in trading arms overseas in breach of sanctions can also have state connections, working for state-trading companies for example. However, there are also many examples of private sector middlemen being motivated purely by profit, having no affinity with the state, and even trying to overcharge those seeking to procure or broker the sale of proliferation-sensitive goods by taking a significant cut.

Organizations providing enabling services such as financial services and transportation can also have connections to the proliferating state – also often bridging the realms of state-ownership and control, and the private sector. State-owned banks have been sanctioned for their role in proliferation financing in the past. Quasi-state transportation assets have also alleged to have been involved in proliferation networks. The operations of these logistical assets are mostly outside of the borders of the proliferating state, and will be considered alongside other state assets below. Having considered definitional issues, the use of state resources needs conceptualization.

### ***Between State Criminality and Routine Activity***

The illicit trade that supplies WMD programs, and involves breach of arms embargos, can constitute criminal activity.<sup>19</sup> How can this criminal activity best be contextualized?

Beyond corruption and embezzlement, elements of states –government officials, members of legislatures, intelligence agencies and the military– have frequently been shown to be involved or have interests in transnational criminal activity.<sup>20</sup> The term “criminal state”, a contested and broad concept, has been coined in the literature to describe a wide variety of states in which the government and other structures have been permeated by criminal



behavior.<sup>21</sup> Miklaucic and Naim have broken down criminal states into a loose typology based on the extent of criminality— from “criminal penetration” of corrupt individuals in governmental structures and networks, “criminal infiltration” constituting penetration with a greater loss of legitimacy, “criminal capture” where the state has lost the ability to counter powerful embedded criminal networks, and finally “criminal sovereignty” where criminal activity becomes a core state mission and resisting complicity is futile.<sup>22</sup>

The criminal activities in these criminal states are largely conducted for the personal financial gain of those involved. For example, corrupt government officials taking bribes, syphoning off funds, or using their position to facilitate personally enriching profitable illicit activities. However, "criminal sovereignty", the most extreme type, involves illicit activity undertaken as a part of, and to further, the policy of the state. North Korea is the most frequently given example of criminal sovereignty, with the state's activities being "unique in the contemporary international security arena", and involving the state effectively maintaining "the monopoly on the conduct of illicit activities".<sup>23</sup> Crimes are committed "beyond the borders of North Korea by the regime itself, not solely for the personal enrichment of the leadership, but to prop up its armed forces and to fund its military programs".<sup>24</sup>

North Korea's criminal sovereignty is driven, organized and facilitated by state resources. This state directed crime has been institutionalized within the ruling party through “Office 39”, and has seen the use of assets not available to non-state actors such as "merchant and military vessels, diplomatic and embassy posts, as well as state run companies and collective farms".<sup>25</sup> However, according to Chestnut, state oversight and control of North Korea's illicit activities has declined since the 1980s and 1990s, as the state has increasingly outsourced drug trafficking and other activities to criminal groups.<sup>26</sup>

The increased use of sanctions as a foreign policy tool has resulted in the growth of sanctions-busting criminal activity, which is often tacitly welcomed or actively enabled by

sanctioned states and third country governments.<sup>27</sup> These are efforts to undermine the effects of economic sanctions and other embargoes, often by smuggling goods to compensate for shortages or to make up for lost trade revenues more broadly. Efforts to bust sanctions, embargoes and circumvent economic measures are as old as these policy tools themselves.<sup>28</sup> More recently, in his piece on the "criminalizing consequences of sanctions", Andreas has emphasized the role that states and government actors have in breaching sanctions, and the wider temporal and geographical effects.<sup>29</sup>

While some states have mobilized state resources in support of illicit activities, all states have mobilized state resources in support of more “legitimate” national security and trade activities. This includes the support of intelligence efforts, procurement, purchase or sales of arms, and broader commercial diplomacy. States routinely use their resources such as embassies in support of intelligence activities.<sup>30</sup> Declared intelligence officers are frequently stationed at embassies to support intelligence networks composed of undeclared "illegals" and their sources.

“Commercial diplomacy” has been an increasingly important function for embassies and diplomatic personnel.<sup>31</sup> This includes in civil commercial areas – obtaining market intelligence, facilitating trade missions and supporting companies from home, and negotiating bilateral commercial agreements—as well as trade in arms.<sup>32</sup> The UN charter enshrines member states' right to self defence, and the procurement of arms to this end is normal and "legitimate".<sup>33</sup> State resources and support is often mobilized to procure and export arms— for example, through use of embassies and intelligence agencies, provision of favorable financial assistance, support of promotion and marketing efforts at trade fairs and use of military personnel, existing military and defence relationships.<sup>34</sup> In some sense, arms exports and procurement are a clear extension of foreign policy, the core mission which embassies and diplomatic corps support.

Therefore, it is argued that the states' use of these state assets in proliferation networks lies somewhere between state criminality and these routine national security and commercial activities. Essentially, while what is illegal or illicit is enshrined in national and international laws, what is "legitimate" is completely in the eye of the beholder.<sup>35</sup> That such activity constitutes state criminality might be the view of states supporting nonproliferation or the implementation of sanctions. However, conversely, in the view of the sanctioned state, broader economic sanctions and embargoes are frequently portrayed as "illegal", "unlawful", "immoral" or unfair.<sup>36</sup> In their view, the use of state resources to breach sanctions through procurement or exports is therefore likely viewed not all too different from other routine activities.

### ***State Resources, "Competitive Advantage" and "Competitive Adaptation"***

In cases where state resources are used to support illicit trade, the sanctions-busting elements of the state, exhibit, or are perceived as providing, a "competitive advantage" over other potential activity providers.<sup>37</sup> In the business world, competitive advantage is defined as an "advantage a firm possesses over its competitors" and takes numerous forms.<sup>38</sup> State resources may have advantages over use of other commercial resources. For example, utilizing diplomats as middlemen might have advantages over private sector brokers or unaffiliated arms dealers; military or state-connected transportation assets might have benefits over commercial providers. In the business world, competitive advantage is generally related to profitability.<sup>39</sup> In relation to illicit trade, profitability sits alongside other factors such as the need to deceive industry, governments and intelligence agencies, and more broadly evade those seeking to prevent illicit transfers.<sup>40</sup>

The competitive advantages held by criminal states have been discussed – especially in relation to territorial control. For example, state criminality allows North Korea to produce narcotics in large quantities because it has the territory to do so, which constitutes an "enforcement free environment".<sup>41</sup> In terms of proliferation networks, Hastings's geographical approach, and discussion of state resources and prerogatives also relates to territorial control, but in the inverse – avoiding reliance on transportation routes or

infrastructure which is not in the proliferating state's control. He notes those with state resources can bypass commercial transportation infrastructure and unfriendly territories, thus making shipments less likely to be compromised.<sup>42</sup>

It should be noted that decision-making regarding illicit network *modus operandi* is not necessarily top-down, and does not necessarily result from a systematic assessment of costs and benefits. The state resources themselves may show propensity to adapt, assume new roles and affect relative competitive advantage. New roles can be driven by personal profit or gain within the system in which they are operating. Taking embassies for example, noting a level of “versatility and adaptability”, Berridge has suggested that “Embassies can fulfil any number of subsidiary functions”, in order to cope with “changing circumstances abroad and a difficult climate at home”.<sup>43</sup> In the North Korean case, since the 1960s embassies and diplomatic missions have been expected to “self-finance”, to send funds back to Pyongyang, and diplomats have been keen to supplement their relatively low salaries.<sup>44</sup> This has created a spate of inventive, innovative, questionable and sometimes criminal schemes being run out of North Korean diplomatic missions.

Efforts by governments, intelligence agencies, industry and other actors seeking to counter proliferation also shape the choices and decisions of those involved in these networks. “Competitive adaptation” refers to how groups learn and adapt in response to the actions of their adversaries.<sup>45</sup> The ongoing process of competitive adaptation has been seen on both sides in a decades-long game of cat and mouse between proliferators and those seeking to stop them. The following section considers the competitive advantage of state resources, and how these relative advantages have evolved over time due to the process of competitive adaptation.

### **State Procurement and Sales Assets: What Competitive Advantages Do They Offer?**

State assets are used in proliferation networks because they can be, and because they have certain specific benefits –or “competitive advantages”– over other options. The following

two sections consider the competitive advantages of these assets as compared to private sector alternatives in two main areas: First, the roles of diplomats and intelligence agencies in procurement and exports in breach of embargoes, relative to private sector middlemen. Second, state and quasi-state logistical assets to physically transfer the goods, as compared to private sector alternatives. The competitive advantages of these assets are not static, therefore these sections also consider the role of competitive adaptation.

Together, these sections argue that the competitive advantage of some state assets – particularly in the area of logistics – has declined. The utility of procurement assets is less likely to change. Diplomatic assets, unlikely to decline in utility due to protocol and privilege, may decline as their use is recognized and if the proliferating state in question is diplomatically isolated by the international community. Intelligence assets may also decline in utility as scrutiny is focused on them, however their clandestine nature means this is less likely to be the case.

### ***Diplomatic Assets***

Embassies and diplomats have long played a role in illicit procurement and sales efforts. Pakistani procurement efforts in the 1970s saw European embassies used to acquire nuclear-related goods. SA Butt, allegedly an accredited diplomat, simultaneously wore “the hats of secretary, consultant, recruiter and distributor”, taking a central role in Pakistan’s procurement network, setting up front companies, coordinating the European visits and activities of scientists and other Pakistani nationals involved in procurement.<sup>46</sup> He operated first in the Pakistani embassy in Brussels, allegedly as the “head of the science and technology department”.<sup>47</sup> Later, Butt operated a small office outside of Paris, allegedly the Embassy’s scientific and technical section of the embassy, and just a three minute walk from major French nuclear company SGN.<sup>48</sup> A separate operation was set up twenty miles outside of Bonn in West Germany in 1977 allegedly by another accredited diplomat –Ikram ul-Haq Khan– with close relations to the Pakistani Embassy in the Federal Republic of Germany.<sup>49</sup> Other sources have suggested the embassy itself in Bonn was also involved.<sup>50</sup>

In short, Pakistan's use of embassies in its procurement operations was "systematic" from the 1970s until at least the late 1990s.<sup>51</sup>

North Korea has continually used diplomats and embassies to support their WMD programs. In the 1990s, a North Korean diplomat based at the country's mission in Vienna –Yun Ho Jin– was allegedly involved in illicit procurement, facilitating North Korean trade delegation visits to Europe, with some technology allegedly being transferred to the Yongbyon nuclear research center.<sup>52</sup> More recently, the UN panel monitoring North Korea's sanctions noted diplomats based in Germany were also involved in efforts to acquire machine tools in the 2000s.<sup>53</sup> As mentioned above, in 2018 a German intelligence official noted that the North Korean embassy in Berlin had been used to acquire missile and nuclear related dual-use goods over the previous two years.<sup>54</sup> Furthermore, in the area of conventional arms, the UN panel has noted that diplomats of the Democratic People's Republic of Korea (DPRK) "or officials travelling on diplomatic or service passports" have helped to facilitate "numerous violations of the arms embargo".<sup>55</sup>

Examples of diplomats and embassies being involved are by no means limited to Pakistan and North Korea. Iran has also allegedly made frequent use of embassies and diplomats in its networks. For example, its Bonn embassy was used in the 1980s for procurement of chemical weapons related goods, and its Beijing embassy was involved in missile-related procurement activities in the 2000s.<sup>56</sup>

Besides the embassies themselves, and departments of them, commercial interest and trade promotion offices, as well as their connections to state-trading companies can also be of use in these networks. The degree to which these offices are connected to the embassy varies – sometimes they are on embassy premises; sometimes those working there have diplomatic privileges and immunities. North Korean diplomats that travelled to Ukraine in 2011, seeking to gain access to "secret academic theses" from a Ukrainian rocket design bureau were accredited to the DPRK's "Trade Representative Office in Belarus".<sup>57</sup> In the 1980s the

Iranian government operated three military service Procurement Offices in London to purchase arms in the face of US efforts to implement an arms embargo. Some of these were initially based on embassy property, and later moved to the National Iranian Oil Company building.<sup>58</sup>

Embassies also have wider utility in supporting proliferation networks – much in the way they might support other commercial activities. It is unlikely a coincidence that arms dealer Michael Ranger notes that he met North Korean arms dealers “...at public places (hotels, restaurants and bars) in third countries where the Democratic People’s Republic of Korea maintained embassies”.<sup>59</sup> North Korean state trading companies involved in the arms trade and other activities are frequently supported by North Korean embassies.<sup>60</sup> In the *Chong Chon Gang* case, where a large shipment of arms was interdicted in Panama on route to North Korea, officials from the DPRK embassy in Cuba were implicated in the transfer by documents left on the ship, and Chinpo Shipping Company, involved in financial transactions, was co-located with the DPRK embassy in Singapore.<sup>61</sup>

Proliferators’ have also used diplomatic bags and other immunities to enable their activities. Iraqi officials allegedly used diplomatic pouches to transfer cash and procurement directives and made use of mission vehicles with diplomatic plates to transfer cash.<sup>62</sup> Pakistani officials used pouches to transfer sensitive documentation related to the nuclear program.<sup>63</sup>

### ***Intelligence Assets***

States frequently utilize their intelligence organizations and assets, acting through their embassies or otherwise, in their procurement or sales activities in breach of sanctions. The Iraqi Intelligence Service (IIS), for example, was heavily involved in illicit procurement of dual-use and military goods for Iraq’s missile and military programs during the 1990s. According to the Iraq Survey Group (ISG), the IIS was used by Saddam to “undertake the most sensitive procurement missions”.<sup>64</sup> IIS operatives were based in most Iraqi embassies

abroad under diplomatic cover and in some cases as commercial attaches, collaborating with the Iraqi Ministry of Foreign Affairs, Military Industrial Commission, Iraqi Atomic Energy Commission and even other countries' intelligence agencies (notably Syria), to procure military and missile related goods and intangibles.<sup>65</sup> IIS officers were purportedly involved in establishing and running Iraqi front companies for procurement purposes.<sup>66</sup>

Other states' networks have also made use of intelligence assets. The Reconnaissance General Bureau (RGB) of North Korea is allegedly involved in much of the illicit sanctions-busting and finance generating activity, including arms sales through front companies.<sup>67</sup> Their involvement in WMD-related procurement has not been publicly recorded, but is certainly possible. Pakistani procurement operations across Europe in the 1970s and 1980s, heavily involving diplomats and embassies, were allegedly "overseen by ISI [Inter-Services Intelligence] field agents operating under the cover of diplomatic postings".<sup>68</sup>

In the Iranian case, rather than intelligence agencies, the Iranian Revolutionary Guard Corps (IRGC) is heavily involved in illicit procurement and illicit arms exports. The UN Iran Panel noted in 2011 that:

Elements of the IRGC are engaged in a wide variety of activities prohibited under United Nations sanctions, including procurement related to the nuclear and ballistic missile programmes, the smuggling of conventional arms and related materiel, and the establishment of front companies to facilitate transit of prohibited items.<sup>69</sup>

Since the mid-1990s the IRGC has transformed beyond a military institution to also constitute a network of political and economic actors.<sup>70</sup> Especially since 2005 –and spurred on by sanctions– the IRGC have seen a "dramatic increase in their economic importance", building on their "arms imports expertise to create a vast network of shadow ports, through which they smuggle a whole range of goods for the Iranian market".<sup>71</sup>



### ***Competitive Advantages and Adaptation?***

In the above examples, diplomats and intelligence agencies are essentially playing the role of procurement agents, middlemen and brokers in the service of the state. These are potentially roles which could be, and often are, played by elements of the private sector in proliferation networks. What advantages and disadvantages could the use of state assets hold in this respect? Both diplomats and intelligence operatives share some advantages in this respect, both because of their state connections, and because both can be based at diplomatic premises.

Both types of asset can allow illicit procurement or sales activities to be kept “close hold” – meaning a minimal number of people are aware of it. Furthermore, for the most part, these assets will be loyal to the state. Their will and ability to keep activities secret, will perhaps trump interests in generating profit which often drives private sector actors. However, it is not so easy to generalize. For example, Vienna-based North Korean diplomat Kim Jong Ryul, was involved in purchasing all types of commodities for the Pyongyang elite, taking a 3% personal cut of each deal. He would later fake his own death and go into hiding for over a decade before telling his story to journalists.<sup>72</sup> Private sector actors can also be keen to keep involvement secret, to avoid punishment or to avoid losing business to competitors.

Both types of asset potentially offer pre-existing resources and networks to exploit. Diplomatic and intelligence networks will likely be in place before the state decides to develop WMD, or is placed under sanction. Use of pre-existing assets could avoid drawing attention like newly deployed assets could. As the ISG has noted, IIS officers already stationed overseas were “in a good position to carry out the mission... without drawing the attention of the international community”.<sup>73</sup> However, in cases where sanctions are levied against procurement entities and other aspects of a proliferating state’s economy, particularly in economies which already have limited trading links, relying on these networks may be a necessity.

The specific location of embassies and intelligence assets –in diplomatic and trading partners– can also be beneficial. Those in countries with strong diplomatic relationships could be of great use in facilitating arms transfers to or from allies. Those based in, or near to, key markets or those lacking oversight –for example the Pakistanis and North Koreans in Europe (as opposed to the US) in the 1980s and 1990s– could be of great utility in WMD-related procurement efforts.

In the broadest sense, embassies provide “physical sanctuaries and political/ diplomatic/ commercial covers” for individuals involved in procurement.<sup>74</sup> The diplomatic status also arguably offers an air of legitimacy, which may detract from or conceal potential illicit activities.<sup>75</sup> Specific aspects of diplomatic protocol also provides advantages. The 1961 Vienna Convention on Diplomatic Relations (VCDR) codified long-standing protocols on the immunity of diplomats on the basis of “functional necessity”: on the grounds that diplomats cannot fulfil their function without these privileges.<sup>76</sup> Diplomats are inviolable, not liable to arrest; exempt from the jurisdiction of the receiving state; and only the sending state may waive this immunity.<sup>77</sup> The immunity received depends on the type of embassy staff in question – diplomats receive the highest level, followed by technical staff.<sup>78</sup> The specific manner in which status is determined is inconsistent between states.<sup>79</sup> In theory, if discovered, diplomats cannot be prosecuted for efforts to illicitly transfer technology to their state program. The VCDR does, however, allow the receiving state to declare the ambassador or other members of the mission *persona non-grata* (PNG).<sup>80</sup> Thus far, there is no evidence to suggest that a diplomat has been declared PNG for proliferation-related activities.

The provisions of the VCDR also potentially provide other opportunities to conceal or transfer incriminating goods. For example, diplomatic premises (embassies for example), diplomat’s residences, and even mission vehicles are immune from search.<sup>81</sup> Diplomatic bags –packages bearing “visible external marks of their character” containing documents or articles for official use– may not be opened on route back to the home capital, other diplomatic residences or when transiting third countries.<sup>82</sup> These have been used

successfully and unsuccessfully to illicitly smuggle a wide range of items –drugs, commodities, art, weapons– and even people.<sup>83</sup> That diplomatic bags could have utility in proliferation-related transfers was recognized early in the nuclear age: a member of the UN International Law Commission noted in 1957, “Although the smuggling of the vital parts of atomic bombs in the diplomatic bag was still confined to the realms of fiction, there was nothing to prevent its becoming an actual fact”.<sup>84</sup> In cases where abuse of the diplomatic bag is possible, the host country has few options: protesting to the mission in question potentially causing a crisis, or terminating the diplomatic relationship completely.<sup>85</sup>

The key competitive advantages of intelligence agencies lie in their established networks, and the skillset held by their operatives – from establishing clandestine networks, clandestine communications, counterintelligence activities and covert action, right down to the tradecraft of its individual operatives. In some sense, intelligence agencies are the most obvious organ of the state to involve in covert efforts to procure or sell technology from overseas. The procurement aspect has significant parallels with existing intelligence missions pursued by certain intelligence agencies, such as industrial espionage.

Processes of competitive adaptation have likely changed the way states use these resources, although this is difficult to prove. Global measures to counter illicit WMD-related exports have developed significantly – especially over the past 14 years since UNSCR 1540 made export controls and other related tools mandatory for states.<sup>86</sup> Private sector actors do still possess advantages: diplomats and intelligence officers do not necessarily have the same understanding of WMD and military technologies, the relevant markets and suppliers that those in the private sector often do. This may make procurement less efficient, resulting in bad deals or procurement of the wrong merchandise, for example. Use of private sector middlemen could also allow for a degree of “plausible deniability” regarding state connections if illicit activity is uncovered.

State assets –embassies and intelligence operatives– have traditionally been a target for other intelligence agencies. This is especially the case for embassies and declared intelligence officers – declared assets that lack the anonymity of the private sector. In recent years in the North Korean case, there has been a heightened awareness of these and other illicit activities conducted by embassies, with the number of missions and their size being reduced by host governments.<sup>87</sup> Increased scrutiny of North Korean embassies as early as the mid-1990s is credited with Ho Jin Yun’s move away from the Vienna mission, and the continuation of his activities through state-owned Namchongang Trading Company, in the late 1990s.<sup>88</sup> This case suggests advantages for Yun’s activity being undertaken through a quasi-state asset, rather than under diplomatic cover. Perhaps his cover in Vienna was blown, or his change in status may be due to other factors entirely.

### **State Transportation Assets: What Competitive Advantages Do They Offer?**

State-owned and state-connected maritime and air transportation assets have frequently been seen in proliferation networks. Those most clearly linked to the state are military assets. Pakistan’s procurement activities in the 1970s and 1980s involved use of military transportation – for example, a particularly large shipment of a gasification and solidification unit, used in the uranium conversion process was moved from Switzerland to Pakistan by a series of Pakistani Air Force C-130 aircraft.<sup>89</sup> President Musharraf allegedly conceded that many of the transfers undertaken by Khan’s sales network utilized similar military transport aircraft.<sup>90</sup> From the 1990s and into the 2000s, these aircraft were also allegedly utilized in Pakistan’s import of missile related components from North Korea.<sup>91</sup>

Other state-connected transportation assets –for example national merchant fleets– have been used to transport proliferation-related and military goods. North Korea’s merchant fleet, limited and highly fragmented in terms of apparent private ownership, is closely connected to the state.<sup>92</sup> Several cases have been seen where North Korea used North Korean-flagged, owned and operated ships to transport large and sensitive cargoes. This was seemingly more common prior to the initiation of the UN sanctions regime in 2006. For example the DPRK-flagged vessel the *Kuwolsan* was interdicted in 1999, and the

DPRK-owned (Cambodian-flagged) *So San* in 2002, both carrying Scud missiles and related goods to Yemen, and Pakistan or Libya, respectively.<sup>93</sup> In 2009, the *Kang Nam-1*, a DPRK-owned and flagged vessel, attempted to transfer a suspicious cargo to Myanmar, but was forced to turn back by US and international pressure.<sup>94</sup>

More recent efforts to transport goods in breach of sanctions have, likely as a result of a process of “competitive adaptation”, sought to make North Korean involvement less obvious. These efforts have included using flags of convenience, and complex networks of entities to complicate ownership. The *MV Light* also attempted to make a delivery to Myanmar in 2011. Under pressure from a US Naval vessel, the Belize-flagged, and China- and Hong Kong-managed and owned vessel returned to North Korea as the *Kang Nam-1* did two years prior.<sup>95</sup> Evidence later emerged that the ship was DPRK-owned and flagged until 2006, and that when the US Navy requested an inspection in 2011, the shipmaster refused to be boarded noting it to be a “vessel of the Democratic People’s Republic of Korea”.<sup>96</sup>

In a second case, the DPRK-flagged and -owned *Chong Chon Gang* was inspected by Panamanian authorities in 2013, and revealed to be carrying 25 shipping containers of arms hidden under 10,000 tons of sugar. The vessel was allegedly transporting the weapons from Cuba to North Korea for refurbishment. Despite the DPRK-ownership and operation, it was noted by the UN panel that:

The employment of so many role-players in support of the ship suggests a network of entities, centrally managed, working together to deflect scrutiny in order to evade sanctions by minimizing the visibility of the Democratic People’s Republic of Korea in transactions.<sup>97</sup>

Iran's merchant fleet –mostly composed of the Islamic Republic of Iran Shipping Lines (IRISL)– despite being highly fragmented in terms of ownership, also has significant state connections.<sup>98</sup> Iranian use of state-connected logistical assets to transport goods in breach of sanctions also appears to exhibit signs of competitive adaptation. IRISL took steps to conceal their activities following its US designation in 2008, and designation of three subsidiaries by the UN in 2010, reflagging and renaming ships, and transferring them to new ownership.<sup>99</sup> Between 2008 and 2012, the around 130 IRISL-linked vessels saw changes in ownership 220 times, were renamed 150 times, and reflagged over 90 times.<sup>100</sup> IRISL was reportedly involved in sanctions violations in “several cases” before 2010.<sup>101</sup> Non-Iranian flagged vessels were also chartered by IRISL to “conceal” illicit activity.<sup>102</sup>

North Korean, Iranian and Pakistani commercial airlines have also been involved in transportation of WMD-related and sanctioned goods. State-owned Air Koryo and Iran Air have allegedly transported shipments of arms, and been implicated in proliferation related transfers.<sup>103</sup> Air Koryo has a fairly limited ability to lift heavy cargo, so in cases where large shipments of very sensitive or valuable items are involved, non-scheduled or chartered flights may be used.<sup>104</sup> Other privately-owned Iranian airlines allegedly have also been implicated in the transfer of arms, possibly with some level of knowledge, and at least with connections to the Iranian regime.<sup>105</sup> Pakistan International Airlines was also allegedly used to transfer WMD-related materials, including uranium hexafluoride (UF<sub>6</sub>) to Libya, and in other unspecified cases involving particularly “sensitive items” in the late 1990s and early 2000s.<sup>106</sup>

More recently, evidence has increasingly suggested that commercial transportation has been used in lieu of state-controlled transportation assets. Particularly, containerized shipping has been used to move WMD-related goods and weapons in breach of sanctions. A 2012 report notes that since the mid-2000s, Iranian and North Korean efforts to import and export goods have increasingly involved shipments being concealed in containers, carried by major liner shipping, foreign owned and flagged, and not under North Korean or Iranian charter.<sup>107</sup>

In the case of North Korea, largely isolated from the major liner routes, shipments are transported to regional ports –especially the nearby Dalian– for transshipment.<sup>108</sup> Both Iran and North Korea developed methods to mislabel and physically conceal the cargo within containers –for example, behind bags of cement, or powdered milk– and also to conceal its origins after the first transshipment in a foreign port.<sup>109</sup> Similarly, recently uncovered networks transferring dual-use goods to North Korea from China – alongside significant quantities of other commodities – have involved large Chinese commercial operators providing procurement and logistical services together.<sup>110</sup>

### ***Competitive Advantage and Adaptation?***

State-connected shipping has some advantages like state procurement assets above: for example, the ability to keep close hold and secretive, without involving a broader range of commercial actors. However, as Hastings argues, the use of state-assets also allows for more direct routing, potentially avoiding hostile territory and interdiction at third country logistical hubs such as ports and airports.<sup>111</sup> The decision between state assets or state-connected transportation assets, or their commercial equivalents, may also be dictated by limitations in capability or available commercial routes. For example, North Korea has little long-range air cargo capability in its military and Air Koryo, and is not directly connected to the main liner shipping routes.

A more recent shift to commercial alternatives may have been driven both by perceived competitive advantages, and the need to adapt. Use of regular commercial services and containerized shipping reduces transportation costs.<sup>112</sup> While it has been argued that proliferators value secrecy over cost concerns, often taking unnecessarily circuitous routes, information obtained by the UN Panel during their investigation into arms dealer Michael Ranger suggests that the DPRK “looks carefully at the bottom line” including transportation, noting that it insists on using nearby ports for transshipment due to cost concerns.<sup>113</sup>

Several factors have likely led proliferators to adapt their transportation methods in response to efforts to counter these networks. Challenges experienced, as illustrated for example by the unsuccessful interdiction of the *So San*, where the US failed to prevent the missiles from reaching Yemen, have resulted in tools such as the 2004 Proliferation Security Initiative (PSI). PSI seeks to facilitate interdictions at sea, and increased scrutiny on air and shipping lines connected to proliferating states. Sanctions on shipping companies and airlines have also meant increased scrutiny of these transportation methods. The UN Iran Panel has alleged that commercial transportation has been adopted by proliferators because of sanctions, both on domestic shipping companies and specific vessels.<sup>114</sup> Proliferators have embraced the anonymity afforded by hundreds of millions of container movements annually, in a similar manner to drug trafficking organizations' use of containerized cargo.<sup>115</sup> The UN North Korea Panel has noted that containerized cargo is "most effective for the concealment of illicit items".<sup>116</sup>

### **Conclusion: Countering State Proliferation Networks**

The use of state resources – diplomatic, intelligence and logistical assets – in proliferation networks is prevalent, yet also under explored in the existing literature. This article has sought to contextualize their use, providing some conceptual treatment of these aspects of proliferation networks. It has argued that states' use of these assets lies between state criminality and the routine use of these assets by all states around the world for customary national security purposes. It has further sought to develop and use the concepts of "competitive advantage" and "competitive adaptation" to systematically explore the use of these assets. In doing so, it has considered the benefits and challenges for the use of these assets relative to private sector equivalents.

The article finds that the advantages of using these assets are not a clear-cut as might be thought, as all these specific types of assets have significant downsides, especially as a



proliferating state's activities are uncovered, and scrutiny increases. Assets on the procurement side –diplomatic and intelligence– will likely have more durable utility than those on the logistical side, whose utility already appears to have declined. Of diplomatic and intelligence assets, intelligence assets are likely to have more enduring value, because of the clandestine nature of their work and networks. Commercial transportation means – and particularly containerized shipping– seem to be becoming more prominent in transferring proliferation-sensitive goods.

The conclusions of this article, besides providing insights into the *modus operandi* of proliferation networks, have implications for nonproliferation efforts. These state-connected aspects of proliferation networks are amongst the most difficult to counter, being highly secretive, allowing activities to be held close by the proliferating state, and with exceptional sensitivities surrounding diplomatic privileges. Efforts to counter the state-connected elements of illicit procurement networks have been, and are likely to be, intelligence-led. Despite their clandestine nature, open source tools have shown great utility across the board. For example, the UN Panels of Experts, which rely heavily on open source information, have been able to uncover significant proliferation-related activities undertaken using state-connected assets. Opportunities are also afforded by open source data for mapping the illicit networks in the often small commercial and diplomatic circles surrounding embassies, and in tracking maritime traffic.<sup>117</sup> More emphasis should be placed by non-governmental researchers on utilizing these capabilities to further explore these networks.

While efforts to prosecute state-connected elements of the networks are unlikely to be successful, other steps such as designations, reducing the sizes of diplomatic missions, and undertaking at-sea interdictions, can have a significant disruptive effect on their activities. The US disruptive counterproliferation toolset has been expanded in recent years, and merits further consideration.<sup>118</sup> Are there further lessons which can be drawn across from efforts to counter other types of transnational crime – for example narcotics trafficking or cyber-crime – which also often involve entities with state connections? Furthermore, the

apparent shift towards commercial and containerized shipping, potentially provides opportunities as well as challenges. Greater efforts to engage the private sector involved in transportation, besides the more traditional engagement activities with dual-use and military exporters, could also be beneficial.

---

<sup>1</sup> For example, the list of proliferating states that have used illicit procurement to develop nuclear programs includes, but is not limited to, China, India, Iran, Iraq, Israel, Libya, North Korea, Pakistan, South Africa, the Soviet Union, and Syria.

<sup>2</sup> See for example Justin Huggler, “North Korea used Berlin embassy to source nuclear technology”, *The Telegraph*, 4 February 2018 (<https://www.telegraph.co.uk/news/2018/02/04/north-korea-used-berlin-embassy-source-nuclear-technology/>)

<sup>3</sup> UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2017/150, 27 February 2017, pp.15, 150.

<sup>4</sup> *Ibid*, p.36.

<sup>5</sup> Alexander Montgomery, “Ring in Proliferation: How to Dismantle an Atomic Bomb Network”, *International Security* 30:2 (Fall 2005), p.172-173.

<sup>6</sup> Aaron Arnold, “A Resilience Framework for Understanding Illicit Nuclear Procurement Networks”, *Strategic Trade Review*, Vol.3, No.4 (Spring 2017) pp.3-23; Daniel Salisbury, ‘Why do Entities Get Involved in Proliferation? Exploring the Criminology of Illicit WMD-related Trade’, *Nonproliferation Review* (2017), Vol.24, No.3-4, pp.297-314.

<sup>7</sup> See for example, allusions to use of embassies in Feroz Khan, *Eating Grass: The Making of the Pakistani Bomb* (Stanford University Press, 2012), p.146; David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (Free Press, 2010) p.22.

<sup>8</sup> Matthew Bunn, ‘Corruption and Nuclear Proliferation’ in Robert I. Rotberg (ed.), *Corruption, Global Security and World Order* (Washington DC, US: Brookings Institution Press, 2009) p.136.

<sup>9</sup> Glenn Anderson, ‘Points of Deception: Exploring How Proliferators Evade Controls to Obtain Dual-Use Goods’, *Strategic Trade Review*, 2:2 (2016), pp.17-18.

<sup>10</sup> Justin V. Hastings, ‘The Geography of Nuclear Proliferation Networks: the Khan Network’, *Nonproliferation Review*, 19:3 (2012), p.432.

<sup>11</sup> *Ibid*, p.432

<sup>12</sup> *Ibid*, p.429.

<sup>13</sup> *Ibid*, p.446. “If they use their own prerogatives and transportation resources, they will likely be able to acquire technology more securely and more quickly”. He does caveat this, noting those that use commercial infrastructure “can more easily cover their tracks” and state resources “run the risk of discovery and sanctions”.

<sup>14</sup> See for example on North Korea: Sheena Chestnut, “Illicit Activity and Proliferation: North Korean Smuggling Networks”, *International Security* 32:1 (2007), p.80-111; Paul Rexton Kan, Bruce Bechtol Jr and Robert M. Collins, “Criminal Sovereignty: Understanding North Korea's Illicit International Activities”, Strategic Studies Institute 2010; Julian Rademeyer, “Diplomats and Deceit – North Korea’s Criminal Activities in Africa”, Global Initiative against Transnational Organized Crime, September 2017. Other sources mention links between other states, and specific parts of states, in organized crime: See for example discussion of Iran and the IRGC: Frederic Wehrey et al. “The Rise of the Pasdaran Assessing the Domestic Roles of Iran’s Islamic Revolutionary Guards Corps”, RAND report, 2009, p.64-66.

<sup>15</sup> See for example on diplomatic status: Yuliya Zabyelina, “The untouchables: transnational organized Crime behind diplomatic privileges and immunities”, *Trends in Organized Crime* 16 (2013) pp.343-357.

<sup>16</sup> For example, financial service providers are not a focus of this article. While there are clearly similar phenomena and causal factors involved in the behavior of these aspects of proliferation networks, the topic is both large and significant, and therefore merits separate treatment.

<sup>17</sup> Clearly, drawing such a clear-cut distinction is not possible (for example, where corruption is rampant, state-resources could be exploited by private sector actors). However, the typology is loose and proposed to help conceptualize different types of assets and resources available to proliferators.

---

<sup>18</sup> For example, see the discussion of behavioral change amongst large Chinese State-Owned Enterprises (SOEs). Daniel Salisbury and Lucy Jones, "Exploring the Changing Role of Chinese Entities in WMD Proliferation", *China Quarterly*, 225 (2016) p.12-14.

<sup>19</sup> With uneven criminalization – despite the UN Security Council's efforts to universally criminalize this activity through UNSC resolution 1540 (2004) and various sanctions resolutions – it is not possible to state that all of this trade is a criminal act. Criminalization has also varied over time, as well as between jurisdictions.

<sup>20</sup> See for example Moisés Naim, "Mafia States: Organized Crime Takes Office", *Foreign Affairs*, 20 April 2012.

<sup>21</sup> See for example Michael Miklaucic and Moisés Naim, "The Criminal State" in Michael Miklaucic and Jacqueline Brewer (eds.), *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington DC, US: NDU Press, 2013), p.155. He notes "the *criminal state* has been used to characterize countries as diverse as North Korea, Russia and Guinea-Bissau".

<sup>22</sup> *Ibid*, p.157-165.

<sup>23</sup> Kan, Bechtol and Colins, "Criminal Sovereignty" p.3. Other examples are sometimes given such as Liberia under warlord Charles Taylor: Miklaucic and Naim, "The Criminal State", p.163-164. It could be argued non-state groups that have *de facto* control of territory and provide some of the functions of a state, such as certain powerful drug cartels, also exercise a kind of criminal sovereignty.

<sup>24</sup> Kan, Bechtol and Colins, "Criminal Sovereignty", p.2.

<sup>25</sup> *Ibid*, p.3.

<sup>26</sup> Chestnut, "Illicit Activity and Proliferation", p.81, p.88. She notes that there is no evidence of this in WMD-related procurement or transfers. However, the recent US actions taken against large sanctions busting networks based in China, both with regard to coal and other commodities and WMD-related goods, may illustrate a shift.

<sup>27</sup> See Peter Andreas, "Criminalizing Consequences of Sanctions: Embargo Busting and Its Legacy", *International Studies Quarterly* 49 (2005), pp.335-360; Bryan Early, *Busted Sanctions: Explaining Why Economic Sanctions Fail* (CA, US: Stanford University Press, 2015)

<sup>28</sup> See for example, R.T. Naylor, *Patriots and Profiteers: Economic Warfare, Embargo Busting, and State-Sponsored Crime* (McGill-Queen's University Press, 2008)

<sup>29</sup> Andreas, "Criminalizing Consequences of Sanctions".

<sup>30</sup> See Michael Herman, "Diplomacy and Intelligence", *Diplomacy and Statecraft* 9:2 (1998) pp.1-22.

<sup>31</sup> G.R. Berridge, *Diplomacy: Theory and Practice 3rd Ed.* (UK: Palgrave Macmillan, 2005) p.119.

<sup>32</sup> *Ibid*.

<sup>33</sup> Examples where this is not the case include states which have been subject to a UN arms embargo. See <https://www.sipri.org/databases/embargoes>.

<sup>34</sup> See Keith Hartley, "The benefits and costs of the UK arms trade", *Defence and Peace Economics*, 11:3 (2000), p.450.

<sup>35</sup> Legality is a complex question, especially in a paper considering multiple cases between countries and across time. Proliferation-related transactions are, and have not always been, illegal. Proliferation networks have clearly sought to exploit loopholes and operate in grey markets where possible.

<sup>36</sup> For example, in 2017 a North Korean representative suggested new UN sanctions were illegal and unlawful. He noted, "My delegation condemns in the strongest terms and categorically rejects the latest illegal and unlawful U.N. Security Council resolution". Stephanie Nebehay, "North Korea warns U.S. of 'greatest pain', rejects sanctions", *Reuters*, 12 September 2017. Iran also frequently described UN and other nonproliferation sanctions as "illegal" – see for example Thom Shanker and William Broad, "Iran denounces UN sanctions and hits back", *New York Times*, 26 March 2007.

<sup>37</sup> The term has been used in relation to NK's illicit activity in Chestnut, "Illicit Activity and Proliferation", p.95.

<sup>38</sup> John Black, Nigar Hashimzade, and Gareth Myles, *A Dictionary of Economics 4th ed.* (Oxford: OUP, 2013)

<sup>39</sup> Some examples include: "more efficient production techniques, brand image, consumer loyalty, and location". *Ibid*.

<sup>40</sup> On deception see Anderson, "Points of Deception"; on the relative importance of keeping illicit transfers of arms or WMD-related goods secret, rather than keeping transportation costs low, see Naylor, *Patriots and Profiteers*, p.238; and Early, *Busted Sanctions*, p.102.

<sup>41</sup> Chestnut, "Illicit Activity and Proliferation", p.95.

<sup>42</sup> Hastings, "The Geography of Nuclear Proliferation Networks", p.432.

- 
- <sup>43</sup> Berridge, *Diplomacy*, p.119.
- <sup>44</sup> See Rademeyer, “Diplomats and Deceit”, p.17-18.
- <sup>45</sup> Michael Kenney, *Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (Penn State University Press, 2006)
- <sup>46</sup> Khan, *Eating Grass*, p.163; Douglas Frantz and Catherine Collins, *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets...And How We Could Have Stopped Him* (NY, USA: Twelve, 2007) pp.41-2 and p.91.
- <sup>47</sup> Accredited according to Steve Weismann and Herbert Krosney, *The Islamic Bomb* (Times Books, 1981) p.182; Accounts vary – suggesting Butt was posted to Brussels from 1973: Shahid-ur-Rehman, *Long Road to Chagai* (self-published, 1999), p.63; 1975 and moved to Paris in 1977: Weissman and Krosney, *Islamic Bomb*, p.182 and Adrain Levy and Catherine Clarke-Scott, *Deception: Pakistan, The United States and the Global Nuclear Weapons Conspiracy* (Atlantic Books, 2007), p.43.
- <sup>48</sup> Weissman and Krosney, *The Islamic Bomb*, p.197.
- <sup>49</sup> Ibid, p.185. Other accounts do not mention accreditation, and suggest he was from AQ Khan’s Special Works Organisation (SWO). See Levy and Clarke-Scott, *Deception*, p.44.
- <sup>50</sup> Egmont Koch, “Wanted...Bomb Business: Nuclear Aid for Pakistan and India” transcript, West German Broadcasting, 1986.
- <sup>51</sup> International Institute for Strategic Studies, *Nuclear Black Markets: Pakistan, A.Q. Khan and the rise of proliferation networks: A net assessment* (London, UK: Routledge, 2007) p.26.
- <sup>52</sup> Albright, *Peddling Peril*, p.154-155.
- <sup>53</sup> UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2013/337, 11 June 2013, p.29.
- <sup>54</sup> Justin Huggler, “North Korea used Berlin embassy to source nuclear technology”, The Telegraph, 4 February 2018 (<https://www.telegraph.co.uk/news/2018/02/04/north-korea-used-berlin-embassy-source-nuclear-technology/>)
- <sup>55</sup> UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2013/337, 11 June 2013, p.25
- <sup>56</sup> Michael R. Gordon with Stephen Engelberg, “A German Concern Sold Chemicals to Iran, U.S. Says”, *New York Times*, 27 June 1989; US Secretary of State, “Continued Assistance to Iran’s Missile Program”, 07STATE111099, 8 August 2007 ([https://wikileaks.org/plusd/cables/09STATE25689\\_a.html](https://wikileaks.org/plusd/cables/09STATE25689_a.html)).
- <sup>57</sup> “The North Korean spies Ukraine caught stealing missile plans”, 1 September 2017, CNN Online, (<https://www.cnn.com/2017/08/24/europe/ukraine-north-korea-spies/index.html>); UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2013/337, 11 June 2013, p.25.
- <sup>58</sup> Gaylord Shaw and William C. Rempel, “Billion-Dollar Arms Search Spans U.S., Globe”, *LA Times*, 4 August 1985.
- <sup>59</sup> UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2013/337, 11 June 2013, p.38.
- <sup>60</sup> See Andrea Berger, *Target Markets: North Korea's military customers in the sanctions era* (RUSI, 2015) p.60.
- <sup>61</sup> UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2014/147, 6 March 2014, p.31.
- <sup>62</sup> Iraq Survey Group, “Regime Finance and Procurement”, 30 September 2004, p.54, 78.
- <sup>63</sup> Khan, *Eating Grass*, p.146.
- <sup>64</sup> Iraq Survey Group, “Regime Finance and Procurement”, 30 September 2004, p.4.
- <sup>65</sup> Ibid, pp.53-83.
- <sup>66</sup> Ibid, p.80.
- <sup>67</sup> See for example, the Glocom case in Malaysia: James Pearson & Rosana Latiff, “North Korea spy agency runs arms operation out of Malaysia, U.N. says”, *Reuters*, 26 February 2017 (<https://www.reuters.com/article/us-northkorea-malaysia-arms-insight/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-u-n-says-idUSKBN1650YE>). The UN has listed the RGB, noting that it trades in conventional arms in breach of sanctions “Sanctions list established and maintained pursuant to Security Council res. 1718 (2006)”, available from: (<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xml/en/dprk-r.xml>)
- <sup>68</sup> Levy and Scott-Clarke, *Deception*, p.43

- 
- <sup>69</sup> “Panel of Experts Established Pursuant to Resolution 1929 (2010) – Final Report”, undated 2011, p.63.
- <sup>70</sup> Elliot Hen-Tov & Nathan Gonzalez, “The Militarization of Post-Khomeini Iran: Praetorianism 2.0”, *Washington Quarterly* 34:1 (2011), p.50.
- <sup>71</sup> Ibid, p.52.
- <sup>72</sup> Julia Damianova, “North Korea's personal shopper has tales to tell”, *LA Times*, 4 April 2010, (<http://articles.latimes.com/2010/apr/04/world/la-fg-north-korea-shopper4-2010apr04>)
- <sup>73</sup> Iraq Survey Group, “Regime Finance and Procurement”, 30 September 2004, p.77.
- <sup>74</sup> Quote taken from a report describing Iraqi activities. Iraq Survey Group, “Regime Finance and Procurement”, 30 September 2004, p.53.
- <sup>75</sup> Yuliya Zabyelina, “Respectable and professional? A review of financial and economic misconduct in diplomatic relations”, *International Journal of Law Crime and Justice* 44 (2016) pp. 88-102
- <sup>76</sup> Leslie Shirin Farhangi, “Insuring against abuse of diplomatic immunity”, *Stanford Law Review* 38:1517, (1986), p.1521.
- <sup>77</sup> See the Vienna Convention, Article 29: “The person of a diplomatic agent shall be inviolable. He shall not be liable to any form of arrest or detention. The receiving State shall treat him with due respect and shall take all appropriate steps to prevent any attack on his person, freedom or dignity”; article 31: “A diplomatic agent shall enjoy immunity from the criminal jurisdiction of the receiving State”; article 32: “The immunity from jurisdiction of diplomatic agents and of persons enjoying immunity... may be waived by the sending State”.
- <sup>78</sup> Consular and service staff do not receive immunity. See U.S. Department of State, “Diplomatic and consular immunity: Guidance for law enforcement and judicial authorities”, June 2015, (<http://www.state.gov/documents/organization/150546.pdf>)
- <sup>79</sup> Zabyelina, “The Untouchables”, p.349.
- <sup>80</sup> Article 9 of the VCDR reads: “The receiving State may at any time and without having to explain its decision, notify the sending State that the head of the mission or any member of the diplomatic staff of the mission is persona non grata or that any other member of the staff of the mission is not acceptable”.
- <sup>81</sup> See article 22 of the VCDR – “The premises of the mission, their furnishings and other property thereon and the means of transport of the mission shall be immune from search, requisition, attachment or execution”; and article 30 “The private residence of a diplomatic agent shall enjoy the same inviolability and protection as the premises of the mission.”
- <sup>82</sup> Article 27 of the VCDR reads: “The receiving State shall permit and protect free communication on the part of the mission for all official purposes”, “The official correspondence of the mission shall be inviolable” and “The diplomatic bag shall not be opened or detained”.
- <sup>83</sup> See Amy Zeidman, “Abuse of the Diplomatic Bag: A Proposed Solution,” *Cardozo L. Rev.* 11 (1989–1990), p.430; and Ashman and Trescott, *Diplomatic Crime: Drugs, Killings, Thefts, Rapes, Slavery & Other Outrageous Crimes!* (Acropolis Books, 1987) pp.190-223.
- <sup>84</sup> “Summary record of the 399th meeting Topic: Diplomatic intercourse and immunities”, A/CN.4/SR.399, Yearbook of the International Law Commission, 1957, vol. I. ([http://legal.un.org/docs/?path=../ilc/documentation/english/summary\\_records/a\\_cn4\\_sr399.pdf&lang=EFS](http://legal.un.org/docs/?path=../ilc/documentation/english/summary_records/a_cn4_sr399.pdf&lang=EFS))
- <sup>85</sup> Zeidman, “Abuse of the Diplomatic Bag”, p.429.
- <sup>86</sup> This has resulted in a large number of states putting in place comprehensive export control systems, or revising existing legislation. United Nations Security Council, resolution 1540, 28 April 2004.
- <sup>87</sup> For example, in 2013, UNSCR 2094 called upon states to “exercise enhanced vigilance over DPRK diplomatic personnel so as to prevent such individuals from contributing to the DPRK’s nuclear or ballistic missile programmes”. United Nations Security Council, resolution 2094, 7 March 2013.
- <sup>88</sup> Albright, *Peddling Peril*, p.156.
- <sup>89</sup> Hastings, “The Geography of Nuclear Proliferation Networks”, p.434.
- <sup>90</sup> Levy and Clarke-Scott, *Deception*, p.387.
- <sup>91</sup> Ibid, p.309, 337.
- <sup>92</sup> The 2014 UN Panel report notes: “Counter to a global trend of concentrated ownership, few [North Korean shipping companies] own more than five... In many cases, shipping companies appear to be formed at the same time as vessels are renamed a reflagged, most likely in order to have a “clean slate” in terms of history and associate links”. The *Chong Chon Gang* is listed as privately owned, documents found on board suggested it to be subordinate to the state Bureau of Maritime Management. This “calls into question the identification of vessels legally owned by “private” companies in the Democratic People’s Republic of Korea”. See UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2014/147, 6 March 2014, p.46



---

<sup>93</sup> Ibid, p.44.

<sup>94</sup> Choe Sang-Hun, "South Korea Says Freighter from North Turns Back", *New York Times*, 6 July 2009.

<sup>95</sup> UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2012/422, 14 June 2012, p.26

<sup>96</sup> UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2013/337, 11 June 2013, p.44

<sup>97</sup> See UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2014/147, 6 March 2014, p.30.

<sup>98</sup> In 2011, at the height of Iran's faceoff with the P5+1 over the nuclear issue, IRISL's over 130 vessels were operated by around 75 companies, "most of which operate just one or only a few vessels". UN Security Council, "Panel of Experts Established Pursuant to Resolution 1929 (2010) – Final Report", undated 2011, p.46-7.

<sup>99</sup> When IRISL was designated by the US in 2008, Stuart Levey, Under Secretary for Terrorism and Financial Intelligence, noted: "Not only does IRISL facilitate the transport of cargo for U.N. designated proliferators, it also falsifies documents and uses deceptive schemes to shroud its involvement in illicit commerce".

<https://www.treasury.gov/press-center/press-releases/Pages/hp1130.aspx>

<sup>100</sup> "Final report of the Panel of Experts established pursuant to resolution 1929 (2010)", S/2012/395, 12 June 2012, p.37-9.

<sup>101</sup> UN Security Council, "Panel of Experts Established Pursuant to Resolution 1929 (2010) – Final Report", undated 2011, p.61.

<sup>102</sup> See the Monchegorsk and Hansa India cases listed in Ibid, pp.48.

<sup>103</sup> Air Koryo allegedly made deliveries of missile-related goods to Beijing for onward shipment to Egypt. See UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2016/157, 24 February 2016, p.32; Iran Air was allegedly involved in transfers of arms to Syria, "Final report of the Panel of Experts established pursuant to resolution 1929 (2010)", S/2013/331, 5 June 2013, p.25; US State Department cables in 2007 suggested ongoing shipments of missile related goods between North Korea and Iran were being transported by Air Koryo, transshipped at Beijing airport onto Iran Air flights – US Secretary of State, "Post Requested to Follow up on Ongoing Matters of Proliferation Concern Raised At APEC by President Bush", 07STATE152317\_a, 3 November 2007, ([https://wikileaks.org/plusd/cables/07STATE152317\\_a.html](https://wikileaks.org/plusd/cables/07STATE152317_a.html)).

<sup>104</sup> A plane searched at Bangkok airport in Thailand and found to be carrying North Korean arms, had been chartered with Air Koryo issuing the airway bill. See UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2010/571, 5 November 2010, p.26.

<sup>105</sup> The 2011 Iran Panel Report noted that "YasAir appears to be a company formed as a civilian arm of the IRGC and that two out of the four cargo aircraft it possesses were transferred from IRGC". "Panel of Experts Established Pursuant to Resolution 1929 (2010) – Final Report", undated 2011, p.60; Mahan Air allegedly was used to transport arms to Syria, see UN Security Council, "Final report of the Panel of Experts established pursuant to resolution 1929 (2010)", S/2013/331, 5 June 2013, p.25

<sup>106</sup> On the UF<sub>6</sub> see Levy and Clarke-Scott, *Deception*, p.365; Gordon Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network* (OUP, 2009), p.22.

<sup>107</sup> Hugh Griffiths and Michael Jenks, "Maritime Transport and Destabilizing Commodity Flows", SIPRI Policy Paper 32., January 2012, p.39. The 2011 UN Iran panel report also notes 5 incidents of non-compliance under UNSCR 1929 saw shipments "carried by well-established foreign carrier vessels or aircraft, such as CMA-CGM, MSC, Korean Air Cargo, and STX Pan Ocean (Singapore)". See "Panel of Experts Established Pursuant to Resolution 1929 (2010) – Final Report", undated 2011, p.48. North Korean cases also involve commercial shipping – the Panel noted this was the case "in almost all cases" in 2012, UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2012/422, 14 June 2012, p.36. Other examples include NK's use of China Shipping Container Lines, Ethiopian Airlines. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2013/337, 11 June 2013, p.39.

<sup>108</sup> At least 6 cases mention Dalian in the North Korean panel reports.

<sup>109</sup> For example, see cement in the Klos C case- UN Security Council, "Final report of the Panel of Experts established pursuant to resolution 1929 (2010)", S/2014/394, 11 June 2014, p.17. "In some incidents studied, after trans-shipment in the first foreign port, no elements would have permitted differentiation of containers originating from the Democratic People's Republic of Korea and stuffed with illicit items from the vast

---

amount of containers originating from the region”. UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2012/422, 14 June 2012, p.38.

<sup>110</sup> John Park and Jim Walsh, ‘Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences’, MIT Security Studies Program Report, August 2016, p. 23.

<sup>111</sup> Hastings, ‘The Geography of Nuclear Proliferation Networks’, p.432.

<sup>112</sup> UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2013/337, 11 June 2013, p.45.

<sup>113</sup> For the argument regarding costs, see Early, *Busted Sanctions*, p.102. Who notes: “the sensitive nature of such transactions increases the value of discretion and/or opacity provided by particular third-party venues above the logistical advantages they offer”. UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2013/337, 11 June 2013, p.45.

<sup>114</sup> Suggested in UN Security Council, “Panel of Experts Established Pursuant to Resolution 1929 (2010) – Final Report”, undated 2011, p.61.

<sup>115</sup> Griffiths and Jenks, “Maritime Transport and Destabilizing Commodity Flows”, p.37-8.

<sup>116</sup> UN Security Council, ‘Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)’, S/2013/337, 11 June 2013, p.45.

<sup>117</sup> For example, the North Korean advert for Li-6 linked to the Beijing embassy and the Glocom case in Malaysia (both mentioned above) were largely uncovered using open sources.

<sup>118</sup> See for example, civil asset forfeiture: Aaron Arnold, “Solving the Jurisdictional Conundrum: How US Enforcement Agencies Target Overseas Illicit Procurement Networks Using Civil Courts”, *Nonproliferation Review*, forthcoming 2018.